

1 **In the Claims:**

2 Claims 1-51 were pending at the time of the Office Action.

3 Claims 1-4, 7-10, 12, 13, 16-21, 23, 24, 26-28, 31-33, 37, 38, 40-42, 45-48
4 and 51 are rejected.

5 Claims 5, 6, 11, 14, 15, 22, 25, 29, 30, 34-36, 39, 43, 44, 49, and 50 are
6 objected to.

7 Please cancel claims 1-4, 7-10, 19-21, 26-28, 31-33, 37, 38, 40-42, and 45-
8 48 without prejudice.

9 Please amend claims 5, 11, 12, 14-18, 22-25, 29, 30, 34-36, 39, 43, 44, 49,
10 50, and 51 as indicated below.

11 Accordingly, claims 5-6, 11-18, 22-25, 29-30, 34-36, 39, 43-44, and 49-51
12 remain pending as shown in the following complete listing of claims:

13
14 **Listing of Claims:**

15
16 Claims 1-4. (Canceled)

17
18
19 5. (Currently amended) An Internet protocol (IP) filter,
20 comprising processor-executable instructions that, when executed on a processor,
21 perform the following steps:

22 monitoring Internet protocol data packets transmitted from one or more
23 clients to a server;

24 obtaining a network address from an IP data packet transmitted by a client;
25

1 processing IP data packets from the client if a Network address that is
2 uniquely associated with the client is stored in a client table;

3 ~~The Internet protocol filter as recited in claim 1, further comprising~~
4 ~~processor-executable instructions that, when executed on a processor, perform the~~
5 ~~following steps:~~

6 if the first Network address is not stored in the client table, retrieving a
7 client limit value from a client limit field, the client limit value indicating a
8 maximum number of unique clients for which IP data packets can be processed;

9 if the number of Network addresses in the client table is greater than or
10 equal to the client limit value, transmitting a signal to each Network address listed
11 in the client table; and

12 if a client at a second Network addresses does not respond to the signal,
13 removing the second Network address from the client table, inserting the first
14 Network address into the client table and processing IP data packets from the first
15 client.

16
17 6. (Original) The Internet protocol filter as recited in claim 5,
18 further comprising processor-executable instructions that, when executed on a
19 processor, perform the following steps:

20 removing the second Network address from the client table; and

21 inserting the first Network address into the client table.

22
23 Claims 7-10. (Canceled)

24
25 11. (Currently amended) A method, comprising:

1 detecting when a current client attempts to establish a connection with a
2 server;
3 determining a unique client identifier that is associated with the current
4 client;
5 determining if a total number of previous clients having access to the server
6 is less than a client limit;
7 determining if the current client has previously been allowed to access the
8 server;
9 providing access to the server if the total number of previous clients having
10 access to the server is less than a client limit;
11 providing access to the server if the total number of previous clients is
12 greater than or equal to the client limit and if the current client has previously been
13 allowed to access the server; and
14 storing the unique client identifier associated with the current client in
15 memory if access is provided to the current client;

16 ~~The method as recited in claim 7,~~ wherein the determining if the current
17 client has previously been allowed to access the server further comprises:

18 transmitting a signal to each previous client that has been allowed to
19 access the server; and

20 determining that the current client has previously been allowed to
21 access the server if at least one of the previous clients fails to acknowledge the
22 signal.

23
24 12. (Currently amended) The method as recited in claim 11[[7]],
25 further comprising:

1 pre-configuring the client limit; and
2 storing the client limit in memory.

3
4 13. (Original) The method as recited in claim 12, wherein the client
5 limit has a pre-defined maximum to which it may be configured.

6
7 14. (Currently amended) A method, comprising:
8 detecting when a current client attempts to establish a connection with a
9 server;
10 determining a unique client identifier that is associated with the current
11 client;
12 determining if a total number of previous clients having access to the server
13 is less than a client limit;
14 determining if the current client has previously been allowed to access the
15 server;
16 providing access to the server if the total number of previous clients having
17 access to the server is less than a client limit;
18 providing access to the server if the total number of previous clients is
19 greater than or equal to the client limit and if the current client has previously been
20 allowed to access the server;
21 storing the unique client identifier associated with the current client in
22 memory if access is provided to the current client;

23 ~~The method as recited in claim 7, further comprising:~~
24 pre-configuring the client limit;
25 encrypting the client limit; and

1 storing the encrypted client limit in memory.

2
3 15. (Currently amended) A method, comprising:

4 detecting when a current client attempts to establish a connection with a
5 server;

6 determining a unique client identifier that is associated with the current
7 client;

8 determining if a total number of previous clients having access to the server
9 is less than a client limit;

10 determining if the current client has previously been allowed to access the
11 server;

12 providing access to the server if the total number of previous clients having
13 access to the server is less than a client limit;

14 providing access to the server if the total number of previous clients is
15 greater than or equal to the client limit and if the current client has previously been
16 allowed to access the server;

17 storing the unique client identifier associated with the current client in
18 memory if access is provided to the current client;

19 ~~The method as recited in claim 7, further comprising:~~

20 retrieving an encrypted client limit; and

21 decrypting the encrypted client limit to derive the client limit.

22
23 16. (Currently amended) The method as recited in claim 15[[7]],
24 wherein the determining the unique client identifier that is associated with the
25

1 current client further comprises identifying an Internet protocol address from a
2 data packet transmitted by the current client.

3
4 17. (Currently amended) The method as recited in claim 15[[7]],
5 further comprising storing the unique client identifiers in a client table in memory.

6
7 18. (Currently amended) The method as recited in claim 15[[7]],
8 wherein the client identifier is a network address.

9
10 Claims 19-21. (Canceled)

11
12 22. (Currently amended) A server that provides access to a limited
13 number of clients, comprising:

14 memory;

15 a network interface configured to handle communications between the
16 server and a plurality of clients;

17 an operating system stored in the memory;

18 a client limit stored in the memory, the client limit denoting a number of
19 unique clients that are allowed to access the server;

20 an IP stack in the memory that is used to process data packets transmitted
21 from clients;

22 a client table in the memory for storing a unique Network address for each
23 client that accesses the server;

24 a communications filter configured to:
25

1 allow access to a first client if the total number of clients that have
2 accessed the server is less than the client limit, or if the total number of clients that
3 have accessed the server is greater than or equal to the client limit and the first
4 client has previously accessed the server;

5 search the client table for a second Network address associated with
6 the first client and determine that the first client has previously accessed the server
7 if the second Network address is found in the client table; and

8 ~~The server as recited in claim 21, wherein the communications filter is~~
9 ~~further configured to~~ determine the second Network address by signaling each
10 Network address listed in the client table and determine that the second Network
11 address is a network address listed in the table that does not acknowledge the
12 signal.

13
14 23. (Currently amended) The server as recited in claim 22[[19]],
15 wherein the client limit is configurable.

16
17 24. (Currently amended) The server as recited in claim 22[[19]],
18 wherein the Communications filter is further configured to signal that the client
19 limit has been exceeded and to deny server access to the first client if the total
20 number of clients that have accessed the server is greater than or equal to the client
21 limit, and the first client has not previously accessed the server.

22
23 25. (Currently amended) A server that provides access to a limited
24 number of clients, comprising:
25 memory;

1 a network interface configured to handle communications between the
2 server and a plurality of clients;

3 an operating system stored in the memory;

4 a client limit stored in the memory, the client limit denoting a number of
5 unique clients that are allowed to access the server;

6 an IP stack in the memory that is used to process data packets transmitted
7 from clients;

8 a client table in the memory for storing a unique Network address for each
9 client that accesses the server; and

10 a communications filter configured to allow access to a first client if the
11 total number of clients that have accessed the server is less than the client limit, or
12 if the total number of clients that have accessed the server is greater than or equal
13 to the client limit and the first client has previously accessed the server;

14 ~~The server as recited in claim 19~~, wherein the client limit is encrypted, the
15 server further comprising a decryption module configured to decrypt the encrypted
16 client limit.

17
18 Claims 26-28. (Canceled)

19
20 29. (Currently amended) A method for providing server access to
21 a limited number of clients, the method comprising:

22 monitoring TCP/IP packets sent from a plurality of clients to a server;

23 obtaining a unique Network address for each client from one or more
24 packets transmitted by the client;

25 storing the Network address of each client that accesses the server;

1 determining if a client limit has been reached; and
2 providing access to a first client upon determining if the client limit has
3 been reached, or upon determining if the first client has previously accessed the
4 server;

5 ~~The method as recited in claim 26,~~ wherein the determining if the first
6 client has previously accessed the server further comprises:

7 sending a signal to each of multiple Network addresses of clients
8 that have accessed the server; and

9 if there is no response to one of the signals, determining that the first
10 client has previously accessed the server using the Network address of the client
11 from which there was no response detected.

12
13 30. (Currently amended) A method for providing server access to
14 a limited number of clients, the method comprising:

15 monitoring TCP/IP packets sent from a plurality of clients to a server;
16 obtaining a unique Network address for each client from one or more
17 packets transmitted by the client;

18 storing the Network address of each client that accesses the server;

19 determining if a client limit has been reached;

20 providing access to a first client upon determining if the client limit has
21 been reached, or upon determining if the first client has previously accessed the
22 server;

23 ~~The method as recited in claim 26, further comprising:~~

24 retrieving an encrypted client limit; and

25 decrypting the encrypted client limit to derive the client limit.

1
2 Claims 31-33. (Canceled)

3
4 34. (Currently amended) An operating system stored on a
5 computer-readable medium, the operating system comprising:

6 an IP stack for processing Internet protocol data packets received from
7 multiple clients;

8 a client limit field containing a client limit value that denotes a maximum
9 number of clients that may access the IP stack;

10 a client table containing a unique Network address for each client that has
11 accessed the operating system; and

12 a communications filter configured to:

13 determine a first Network address of a first client attempting to
14 access the operating system, search the client table for the first Network address,
15 and allow the first client to access the operating system if the first Network
16 address is found in the client table;

17 allow the first client to access the operating system if the number of
18 Network addresses in the client table is greater than or equal to the client limit
19 value and the first client has previously accessed the operating system using a
20 second Network address that is stored in the client table;

21 ~~The operating system as recited in claim 33, wherein the communications~~
22 ~~filter is further configured to:~~

23 ~~transmit a signal to each Network address listed in the client table;~~

24 ~~monitor for an acknowledgement to each signal; and~~
25

1 if an acknowledgement is not received from a network address in the
2 client table, determining that the non-acknowledging Network address is the
3 second Network address used by the first client.

4
5 35. (Original) The operating system as recited in claim 34, wherein
6 the Communications filter is further configured to replace the second Network
7 address in the client table with the first Network address.

8
9 36. (Currently amended) An operating system stored on a
10 computer-readable medium, the operating system comprising:

11 an IP stack for processing Internet protocol data packets received from
12 multiple clients;

13 a client limit field containing a client limit value that denotes a maximum
14 number of clients that may access the IP stack;

15 a client table containing a unique Network address for each client that has
16 accessed the operating system; and

17 a communications filter configured to determine a first Network address of
18 a first client attempting to access the operating system, search the client table for
19 the first Network address, and allow the first client to access the operating system
20 if the first Network address is found in the client table;

21 ~~The operating system as recited in claim 31,~~ wherein the client limit value
22 is encrypted, and the operating system further comprises a decryption module that
23 is configured to decrypt the client limit value.

24
25 Claims 37-38. (Canceled)

1
2 39. (Currently amended) A computer-readable medium
3 comprising computer-executable instructions that, when executed on a computer,
4 perform the following steps:

5 determining a first Internet Protocol (IP) address transmitted from a first
6 client to a server;

7 searching a client table for the first Network address;

8 allowing the first client to access the server if the first Network address is
9 found in the client table;

10 ~~The computer-readable medium as recited in claim 37, further comprising~~
11 ~~computer-executable instructions that, when executed on a computer, perform the~~
12 ~~following steps:~~

13 transmitting a signal to each Network address listed in the client table; and
14 if there is no response from one of the Network addresses signaled,
15 allowing the first client to access the server, removing the non-responsive Network
16 address from the client table, and inserting the first Network address into the client
17 table.

18
19 Claims 40-42. (Canceled)

20
21 43. (Currently amended) A computer system, comprising:

22 a processor;

23 a network interface card to handle communications with multiple clients;

24 memory;

25 a global system registry;

1 a client table having one entry for each client allowed to access the system,
2 each entry including a unique Internet protocol (IP) address for each client; and
3 a communications filter configured to:
4 retrieve a client limit from the global system registry;
5 determine a first Network address that is associated with a first client
6 attempting to access the system;
7 allow the first client to access the system if the first Network address
8 is stored in the client table or if the number of client table entries is less than the
9 client limit;
10 store the first Network address in the client table if the first client is
11 allowed to access the system;
12 allow the first client to access the system if the number of entries in
13 the client table is greater than or equal to the client limit and if the first client has
14 previously accessed the system; and

15 ~~The computer system as recited in claim 41, wherein the Communications~~
16 ~~filter is further configured to~~ determine if the first client has previously accessed
17 the system by transmitting a signal to each Network address listed in the client
18 table, monitoring responses to the signals to determine if a client at a second
19 Network address is no longer using the Network address, substituting the first
20 Network address in the table for the second Network address and allowing the first
21 client to access the system if the client at the second Network address does not
22 respond to the signal.

23
24 44. (Currently amended) A computer system, comprising:
25 a processor;

1 a network interface card to handle communications with multiple clients;
2 memory;
3 a global system registry;
4 a client table having one entry for each client allowed to access the system,
5 each entry including a unique Internet protocol (IP) address for each client; and
6 a communications filter configured to:
7 retrieve a client limit from the global system registry;
8 determine a first Network address that is associated with a first client
9 attempting to access the system;
10 allow the first client to access the system if the first Network address
11 is stored in the client table or if the number of client table entries is less than the
12 client limit; and
13 store the first Network address in the client table if the first client is
14 allowed to access the system;

15 ~~The computer system as recited in claim 40,~~ wherein the client limit is
16 encrypted, the computer system further comprising a decryption module
17 configured to decrypt the encrypted client limit.

18
19 Claims 45-48. (Canceled)

20
21 49. (Currently amended) A communications protocol filter,
22 comprising processor-executable instructions that, when executed on a processor,
23 perform the following steps:

24 monitoring communications protocol data packets transmitted from one or
25 more clients to a server;

1 obtaining a network address from a communications protocol data packet
2 transmitted by a client;

3 processing communications protocol data packets from the client if a
4 Network address that is uniquely associated with the client is stored in a client
5 table;

6 ~~The communications protocol filter as recited in claim 45, further~~
7 ~~comprising processor-executable instructions that, when executed on a processor,~~
8 ~~perform the following steps:~~

9 if the first Network address is not stored in the client table, retrieving a
10 client limit value from a client limit field, the client limit value indicating a
11 maximum number of unique clients for which communications protocol data
12 packets can be processed;

13 if the number of Network addresses in the client table is greater than or
14 equal to the client limit value, transmitting a signal to each Network address listed
15 in the client table; and

16 if a client at a second Network addresses does not respond to the signal,
17 removing the second Network address from the client table, inserting the first
18 Network address into the client table and processing communications protocol
19 data packets from the first client.

20
21 50. (Original) The communications protocol filter as recited in claim
22 49, further comprising processor-executable instructions that, when executed on a
23 processor, perform the following steps:

24 removing the second Network address from the client table; and

25 inserting the first Network address into the client table.

1
2 51. (Currently amended) The communications protocol filter as
3 recited in claim 49[[45]], wherein the communications protocol is an Internet
4 protocol and the communications protocol data packets are Internet protocol data
5 packets.
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25